

FILED  
SCRANTON

JUL 30 2021

PER                       
DEPUTY CLERK

**UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA *EX*  
*REL.* TERRALYN WILLIAMS  
SEILKOP,

Plaintiffs,

vs.

INSIGHT GLOBAL, LLC

Defendant.

**FILED *IN CAMERA* AND UNDER  
SEAL PURSUANT TO THE  
FALSE CLAIMS ACT, 31 U.S.C.**

**DO NOT PLACE ON PACER  
DO NOT PLACE IN PRESS**

Case No. \_\_\_\_\_

---

**COMPLAINT FILED *IN CAMERA* AND UNDER SEAL PURSUANT TO  
THE FALSE CLAIMS ACT, 31 U.S.C. § 3729 *ET SEQ.***

---

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	JURISDICTION & VENUE.....	3
III.	PARTIES.....	3
IV.	LEGAL BACKGROUND .....	5
A.	The False Claims Act, 31 U.S.C. § 3729 et seq. ....	5
V.	FACTUAL BACKGROUND .....	8
A.	Defendant Created A Contact Tracking System Without Any Security Protections .....	15
1.	Defendant Knowingly Failed To Place Adequate Safety Controls On Data, And Knowingly Risked Unauthorized Data Access When It Contracted With DOH And During Performance Of The Contract .....	19
B.	Defendant Failed To Track Data In A Valid, Relevant or Useful Manner, Resulting In Worthless Data Reporting To DOH.....	26
C.	Defendant Constructively Discharged Ms. Seilkop .....	30
VI.	LEGAL CAUSES OF ACTION .....	31
VII.	PRAYER FOR RELIEF.....	33

## **I. INTRODUCTION**

1. Terralyn Williams Seilkop (“Relator”), by and through her attorneys, files this Complaint, in camera and under seal, pursuant to the False Claims Act (“FCA”), 31 U.S.C § 3729 et seq., against Insight Global, LLC (“Insight” or “Defendant”) to obtain redress on behalf of the United States for Defendant’s FCA violations resulting from its fraudulent inducement of the Pennsylvania Department of Health (“DOH”) to enter a contract with Defendant that was funded by the United States Department of Health and Human Services (“HHS”), by and through, among others, the Centers for Disease Control (“CDC”), and false claims Defendant submitted to DOH for payment or approval.

2. On or about July 29, 2020, Defendant entered into an approximately five-month, \$23 million contract with the DOH to perform Pennsylvania’s Covid-19 contact tracing functions. The contract required Defendant, among other things, to create computer systems that could securely store and manage patients’ protected health information (“PHI”) and personally identifiable information (“PII”), and to use professional means to protect this data from unauthorized access. The contract also required Defendant to provide services that would trace and track Covid-19 in Pennsylvania.

3. Aware that the contract obligated it to provide secure computer systems that were protected from improper or illegal access, Defendant entered into the contract with DOH aware that it did not have in place, nor intend to purchase and/or use, computer software and other computer security systems to prevent access to the PHI and PII.

Instead, Defendant knowingly used free computer programs that permitted the general public to access the PHI and PII obtained from Pennsylvania Covid-19 victims.

4. Relator served as Defendant's Business Intelligence Reporting Manager and repeatedly warned Defendant, verbally and in writing, of its obligations to provide secure computer systems, but Defendant knowingly ignored Relator and failed to take any actions to protect PHI and PII, placing Pennsylvania residents in danger of privacy invasions.

5. When pressed by Relator, Defendant stated that it was not willing to pay for the necessary computer security systems and instead preferred to use its contract funds to hire large numbers of workers. Defendant would make a profit from a percentage of an employee's pay but could not recoup its costs, or make a profit, for the purchase of computer security systems.

6. In January 2021 after Relator's repeated complaints, Defendant made minor changes to its system that still failed to adequately protect PHI and PII data from unauthorized access. Further, Defendant failed to secure the data obtained from August 2020 to January 2021, that was still readily accessible to the general public. As late as May 2021, the pre-January 2021 data was still readily accessible to the general public.

7. Defendant's work product produced data that was not valid, relevant or searchable. Thus, Defendant failed even to trace or track Covid-19 in Pennsylvania, which was its primary duty under the contract.

8. At the time of contract formation, Defendant knowingly failed to obtain any computer security to meet its contractual obligations. Defendant's actions fraudulently induced DOH to enter into the contract with Defendant. Defendant then submitted claims for payment for its services, knowingly falsifying that it had provided the contractually required services. Defendant was paid using CDC funds for its insufficient and improper services.

9. As a result of Defendant's actions, the United States has been damaged.

## **II. JURISDICTION & VENUE**

10. Jurisdiction is founded upon the FCA, 31 U.S.C. §§ 3729 *et seq.*, specifically, 31 U.S.C. §§ 3732(a) & (b), and 28 U.S.C. §§ 1331 and 1345.

11. The Court may exercise personal jurisdiction over Defendant because it transacts business in this District and engaged in the alleged illegal activities and practices in this District.

12. Venue in this District is appropriate under 31 U.S.C. § 3732(a) in that many of the acts complained of took place in this District.

## **III. PARTIES**

13. The United States is the real party in interest to the claims in this action. Through

HHS, CDC administers some of the emergency programs necessitated by the novel coronavirus Covid-19 pandemic.

14. In approximately May 2020, DOH received a grant from the CDC for, among other uses, contact tracing of the Covid-19 virus. The total grant amount was approximately \$66 million.

15. Relator Terralyn Williams Seilkop (“Relator” or “Ms. Seilkop”) is a resident of Florida, and was formerly Defendant’s Business Intelligence Reporting Manager on the DOH project, working as a 1099 contractor.<sup>1</sup> Relator was responsible for managing data created by contact tracers interacting with Pennsylvania residents who had been infected with Covid-19. Ms. Seilkop worked for Defendant from approximately October 22, 2020 until January 8, 2021.

16. Insight Global, LLC (“Insight” or “Defendant”), headquartered in Atlanta, GA, was founded in 2001 and incorporated in Delaware in 2007. In 2010, Harvest Partners, a private equity firm headquartered in New York, New York, purchased Insight. Touting itself to be one of the top five providers of information technology, accounting, finance and engineering staffing solutions throughout North America, Defendant has 44 offices from which it provides temporary and permanent staffing placements for Fortune 500

---

<sup>1</sup> Upon information and belief, all persons working for Defendant on the DOH contract were independent contractors and not employees. These persons are referred to throughout as “workers.”

corporations. Bert Bean is the chief executive officer of Insight, and Harvest has a senior team managing Insight.

17. Christopher McKay was Defendant's project manager on the DOH data-centric managed services contract. McKay was a service delivery executive for Defendant from July 2019 to May 2021. McKay states on LinkedIn that he launches strategies for customer service organizations and small businesses by implementing process improvements. McKay has no experience with IT or creating secure databases.

#### **IV. LEGAL BACKGROUND**

##### **A. The False Claims Act, 31 U.S.C. § 3729 et seq.**

18. The False Claims Act establishes liability for any person who knowingly presents, or causes to be presented, to the United States a false or fraudulent claim for payment or approval, 31 U.S.C. § 3729(a)(1)(A); or any person who knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim, 31 U.S.C. § 3729(a)(1)(B).

19. The term "knowingly" under the FCA means that a person, with respect to information, (i) has actual knowledge of the information, (ii) acts in deliberate ignorance of the truth or falsity of the information, or (iii) acts in reckless disregard of the truth or falsity of the information. 31 U.S.C. § 3729(b)(1). No proof of specific intent to defraud

is required to show that a person acted knowingly under the FCA. 31 U.S.C. § 3729(b)(1)(B).

20. Section 3729(a)(1) of the FCA provides that a person found to have violated the FCA is liable to the United States Government for three times the amount of damages that the Government sustains because of the act of that person, plus a civil penalty of no more than \$23,331 and no less than \$11,665 for each violation occurring after November 2, 2015. 31 U.S.C. § 3729(a)(1), 28 C.F.R. § 85.5 (2020).

21. “Fraudulent inducement” means that FCA liability will attach to each claim submitted to the government under a contract, when the contract, loan guarantee or other agreement was originally obtained through false statements or fraudulent conduct. U.S. ex rel. Thomas v. Siemens AG, 991 F.Supp.2d 540, 567-68 (E.D. Pa. 2014).

22. False claims are either factually or legally false. A factually false claim misrepresents what goods or services are provided to the Government. A legally false claim occurs when a claimant knowingly falsely certifies that it has complied with a contract, statute or regulation material to the Government’s payment decision. U.S. ex rel. Wilkins v. United Health Group, Inc., 659 F.3d 295, 305 (3d Circ. 2011).

23. For a false claim to be material, it must have a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property. Universal Health Services, Inc. v. U.S. ex rel. Escobar, 136 S.Ct. 1989, 2001-2002 (2016).

24. The FCA contains a public disclosure bar, which permits a court to

dismiss an action or claim under this section, unless opposed by the Government, if substantially the same allegations or transactions as alleged in the action or claim were publicly disclosed - (i) in a Federal criminal, civil, or administrative hearing in which the Government or its agent is a party; (ii) in a congressional, Government Accountability Office, or other Federal report, hearing, audit, or investigation; or (iii) from the news media, unless the action is brought by the Attorney General or the person bringing the action is an original source of the information.

31 U.S.C. § 3730(e)(4)(A).

25. A public disclosure only occurs when the allegations and transactions alleged in the complaint are substantially similar to the allegations and transactions of the fraud revealed in the public disclosure. The two documents must be examined on a claim-by-claim basis using a fact-specific analysis. Sturgeon v. Pharmerica Corp., 438 F.Supp.3d 246, 263-264 (E.D. Pa. 2020).

26. The FCA permits a relator to proceed when a public disclosure has occurred if the relator is an original source. "Original source"

means an individual who either (i) prior to a public disclosure under subsection (e)(4)(a), has voluntarily disclosed to the Government the information on which allegations or transactions in a claim are based, or (2) who has knowledge that is independent of and materially adds to the publicly disclosed allegations or transactions, and who has voluntarily provided the information to the Government before filing an action under this section.

31 U.S.C. § 3730(e)(4)(B).

27. On April 29, 2021, several news sources reported that Defendant caused a potential data breach related to its contact tracing work for DOH, potentially involving 72,000 people. On May 5, 2021, a group of plaintiffs filed a class action lawsuit against

Defendant and the DOH related to the potential data breach. Neither of these documents are public disclosures because neither contain the allegations and transactions of the fraud alleged herein.

28. Even if these occurrences are held to be public disclosures, Relator is an original source in that she has knowledge that is independent of and materially adds to any allegedly publicly disclosed allegations or transactions and has voluntarily provided the information to the Government before filing an action under this section.

## **V. FACTUAL BACKGROUND**

29. On or about January 31, 2020, the United States declared a public health emergency to aid the nation's response to the novel coronavirus, later known as Covid-19. On March 13, 2020, a national emergency was declared due to the extensive spread of Covid-19, as it is a highly contagious disease.

30. Beginning in March 2020, Congress passed several laws to fund a nationwide response to Covid-19. These laws, among other things, provided funds to the CDC to aid in the response to Covid-19, including funding for nationwide contact tracing. In May 2020, the CDC provided grants to states, including Pennsylvania, for purposes of assisting efforts to limit the spread of Covid-19, including contact tracing.

31. Contact tracing is a core public health tool used to interrupt the transmission of

pathogens like COVID-19. Contact tracing staff contact patients to help them recall everyone with whom they have had close contact during the timeframe during which they may have been infectious. Staff then rapidly notify these individuals (close contacts) of their potential exposure to an unidentified patient with the infection.<sup>2</sup> Potentially exposed persons are provided information to understand their risk of contracting the pathogen. Timely contact tracing is critical to effectively slowing or stopping the spread of pathogens.

32. In 2020, Defendant, a staffing agency, sought to expand its business lines by providing data-centric managed services, where Defendant could manage both the staff performing tasks and the data and IT security services. In or around May 2020, Defendant became aware that DOH was seeking data-centric managed services, and, upon information and belief, submitted a proposal to provide those services to DOH. Several other similar companies also discussed their services and proposals with DOH.

33. On July 31, 2020, DOH announced that, without a competitive bidding process, it had entered a five-month \$23 million contract with Defendant to perform contact tracing services for Pennsylvania. Then-Pennsylvania Secretary of Health Rachel Levine announced that this contract was let in order to “bolster and diversify our public health

---

<sup>2</sup> Staff cannot identify the infected person to an exposed person due to Health Insurance Portability and Accountability Act (“HIPAA”) privacy rules.

workforce all while coordinating and mobilizing efforts in order to conquer any potential surge in COVID-19 cases.”<sup>3</sup>

34. Secretary Levine stated that “Insight Global was chosen for their ability to operationalize a large-scale, well-resourced program quickly and efficiently while incorporating diversity and equity in hiring practices, engagement and training of the workforce, and sustainability of the skills developed to create lasting change in the public health and human service workforce.” Id.

35. As part of the announcement, DOH acknowledged that the contract was funded by “nearly \$23 million” of Federal CDC funding. Upon information and belief, these funds were part of the \$66,616,309 CDC granted to Pennsylvania on May 19, 2020 for Covid-19 related services.

36. The contract (attached hereto as Exhibit A) compensated Defendant based on a time and materials basis for the services outlined in the Statement of Work. See, Exhibit A, page 28, ¶ IV.A. The Statement of Work incorporated the DOH HIPAA requirements. Id. at page 30, ¶ VIII. Upon information and belief, Defendant obtained extensions and/or addendums to this contract, permitting it to bill and receive over \$29 million of CDC grant funds for its services to DOH up to and including July 31, 2021.

37. Because of Pennsylvania’s announcements, among other things, Defendant knew that its contract was funded by federal CDC funds.

---

<sup>3</sup> <https://www.media.pa.gov/pages/Health-details.aspx?newsid=938>.

38. Defendant began providing contact tracing services to DOH on or before August 1, 2020. Defendant placed managers on the DOH contract with little to no information technology (“IT”) credentials, such as McKay, Greg Eger (an operations manager in addiction recovery centers) and Shannon Hughes (an operations manager in public health companies with a master’s degree in public health and certifications in project management).

39. The contract required Defendant to, as Secretary Levine stated, “operationalize a large-scale, well-resourced program quickly and efficiently” by providing confidential and secure computer systems where a Covid-19 patient’s PHI and PII data, and data from potentially exposed persons, could be stored. The data was then to be used to create reports tracking the spread of Covid-19 in Pennsylvania, to aid public health response to the disease.

40. The contract required Defendant to “recognize and accept[] that the contact tracing workforce will have access to personal health information of contact tracing subjects and must ensure that and all other such information related to the service being provided must be kept confidential and secure.” See, Exhibit A, Contract, 25, at Statement of Work, I.B.iv.

41. The contract also required Defendant to “deploy computing devices for the term of the contract, with encrypted hard drives, disabled read/write capabilities, antivirus software and USB headsets.” See, *Id.*, Statement of Work, I.B.i.

42. The contract, which classifies Defendant as a “business associate,” obligates the Defendant to

establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by [the agreement between Pennsylvania and Defendant] that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI that is created, received, maintained or transmitted on behalf of the [DOH] as required by Subpart C of 45 CFR Part 164. Appropriate safeguards shall include but are not limited to implementing:

- i. administrative safeguards required by 45 CFR 164.308,
- ii. physical safeguards as required by 45 CFR 164.310,
- iii. technical safeguards as required by 45 CFR 164.312, and,
- iv. policies and procedures and document requirements as required by 45 CFR 164.316.

See Exhibit A at 32, Commonwealth of Pennsylvania Business Associate Appendix 1, Health Insurance and Portability and Accountability Act (HIPAA) Compliance (hereinafter, HIPAA Compliance Appendix), Section 5.b.

43. “Administrative safeguards” as defined in 45 C.F.R. § 164.308(a) require a business associate (such as Defendant here) to provide risk management services by implementing “security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level” that will allow the business associate to assess “the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.”

44. The administrative safeguards also require business associates to “implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic [PHI]...and to prevent those workforce members who do

not have access...from obtaining access to electronic [PHI].” 45 C.F.R.

§ 164.308(a)(3)(i). Business associates are also required to “[i]mplement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends...” 45 C.F.R. § 164.308(a)(3)(ii)(c).

Business associates must create “procedures for creating, changing and safeguarding passwords.” 45 C.F.R. § 164.308(a)(5)(i)(D).

45. Pursuant to its DOH contract, Defendant was required to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic [PHI] to allow access only to those persons or software programs that have been granted access rights...” 45 C.F.R. § 164.312(a)(1). Such policies must include assigning each user “a unique name or number for identifying and tracking the user’s identity,” instituting “a mechanism to encrypt and decrypt electronic [PHI],” “implement[ing] procedures to verify that a person or entity seeking access to electronic [PHI] is the one claimed,” “implement[ing] technical security measures to guard against unauthorized access to electronic [PHI] that is being transmitted over an electronic communications network,” and “implement[ing] a mechanism to encrypt electronic [PHI] whenever deemed appropriate.” 45 C.F.R. § 164.312(a)(2), (d) and (e).

46. 45 C.F.R. § 164.410 requires a business associate to treat a data security breach as “discovered”

as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate.

A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

45 C.F.R. § 164.410(a)(2).

47. The contract requires the business associate to notify DOH

within two (2) days of discovery of any use or disclosure of PHI not provided for or allowed by this Agreement, including breaches of unsecured PHI as required by 45 CFR 164.410...An improper use or disclosure or Breach shall be treated as discovered by the Business Associate on the first day on which it is known to the Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred.

See, Exhibit A, at 32, HIPAA Compliance Appendix, Section 5.c.

48. Pennsylvania may terminate the contract if it “determines, in its sole discretion that the Business Associate has violated a material term of this Appendix.”

See, Exhibit A, at 34, HIPAA Compliance Appendix, Section 5.r.

49. Upon information and belief, Defendant obtained a contract extension, amendment, or new contract with DOH for the period of January 1, 2021 to July 31, 2021. This belief is based on the fact that the DOH publicly stated that the contract end date was July 31, 2021.

50. Defendant knew at the time it entered into the contract that it did not have mechanisms in place to adequately secure data. In October 2020 and December 2020, Ms. Seilkop notified Defendant that an improper use equivalent to a data breach had

occurred due to Defendant's failure to purchase security programs or only permit secure access to the data. Defendant took no actions to rectify this situation, nor did Defendant notify DOH of this improper usage and/or actual or potential data breach.

51. On April 29, 2021, Defendant and the DOH publicly announced that some of the PHI and PII that Defendant had collected for over 72,000 people may have been accessible to persons beyond authorized workers and public health officials. Shortly thereafter, on May 10, 2021 DOH announced that it would not renew Defendant's contract when it ended on July 31, 2021.

52. On May 20, 2020, DOH terminated its contract with Defendant effective June 19, 2021, or 42 days before the contract's expiration.

53. From approximately July 2020 until at least July 2021, Defendant submitted invoices or claims for payment to DOH. DOH paid Defendant in response to these claims, with funds granted to DOH from the CDC.

**A. Defendant Created A Contact Tracking System  
Without Any Security Protections**

---

54. Ms. Seilkop's job, as a business intelligence reporting manager, required her to use Covid-19 PHI and PII data recorded by contract tracers, aggregate the data,<sup>4</sup> then run reports based on searches of the aggregated data. Ms. Seilkop was the only business intelligence reporting manager on the project and did not manage any workers.

---

<sup>4</sup> Data aggregation is the process where raw data is gathered and expressed in a summary form for statistical analysis.

55. Upon starting work for Defendant in October 2020, Ms. Seilkop realized that Defendant was not performing its contractually obligated functions. Ms. Seilkop observed that Defendant had failed to provide a secure and confidential computer system or network to protect and store the data obtained by contract tracers.

56. All data obtained by the contact tracers, which contained PHI and PII, were placed in documents housed on Google Docs. Google Docs is Google's browser-based word processor, allowing multiple persons to collaboratively create, edit and share documents online, accessing them from any computer with an internet connection. Google Docs is free and easy to access. There are no built-in security features to prevent anyone with access to Google, or to the documents, to download or disseminate the documents and information stored on Google Docs. It is easily hackable.

57. One person initially creates a document on Google Docs. That person may then share the document with others by sending, via email, a link to the original document. Once the link is sent, the document is not restricted and can be accessed by anyone receiving the link. Defendant's documents were sent to workers via a link permitting access to the documents without any additional layer of security, using the "anyone with the link" setting that permitted all of Defendant's workers to access the Google Docs.

58. This setting permits literally anyone with the link, or anyone able to guess the link's address, to access and download those documents onto their own computer. As long as a person had the link to one document, they could access all of Defendant's

documents, including those containing PHI and PII. This also meant that anyone who hacked a user's emails, or cleverly figured out the link address,<sup>5</sup> could access every document and the PHI and PII. Since there were over a thousand contact tracers, who were regularly coming and going, the likelihood of impermissible access was high, especially given the fact that Google Docs lacked any security process to stop such access.

59. Defendant not only failed to secure the documents containing contact tracing PHI and PII data, it further compromised its security (and increased the risk of hacking) by creating only one username and password for each Google Docs document. There were three main Google Docs documents, and each document had its own username and password. Thus, a single username and password was shared by everyone working on one particular Google Docs document, allowing access to the document's PHI and PII.

60. In order to access Google Docs, a user has to create a personal Google account. When a user logs on to their personal Google account, saving their personal Google username and password (which many users do), then logs on to Defendant's Google docs, another person logging on to the Google Docs documents could also access the first user's saved personal Google username and password, and could access the saved usernames and passwords for any of the first user's other personal accounts. If the first

---

<sup>5</sup> In April 2021, a local reporter hired a computer expert who was able to access the documents by guessing the link's address, without knowing or possessing the actual link.

user exited by simply closing the windows in which Google and Google Docs had been viewed without first logging off, any subsequent user of Defendant's Google Docs documents could access all of the first user's personal accounts. This unsecure situation is inherent in Google Docs.

61. Defendant required its workers to communicate using the unsecured messaging app Slack. For instance, workers sent messages to other workers via Slack with links that provided access to documents on Google Docs. Defendant's use of Slack provided another unsecure means of access to confidential PHI and PII.

62. The most basic means of protecting confidential information is to ensure that only authorized persons have access to the information. Securing access to only authorized users requires the use of secure passwords, secure messaging systems, and document storage sites that provide additional layers of security. Individual, strong and secure passwords limit access to persons who are authorized to use or access a computing program or device and reduce the likelihood of access by unauthorized persons. Computer programs may also have a superuser, or administrator, who can control access and prevent outsiders from gaining access. The administrator can place additional levels of security upon each individual user's account. Hackers able to guess the superuser's password can gain control over multiple user accounts.

63. Defendant lacked basic internet and data security, such as the use of a secure

password system, a secure superuser account, and secure data storage sites. Defendant's failure to secure its data and control access to the data existed from at least late July 2020 and continued until at least May 2021. As late as May 2021, workers could still access the system using the username and password they had obtained, and hackers could still access the information stored on Google Docs.

**1. Defendant Knowingly Failed To Place Adequate Safety Controls On Data, And Knowingly Risked Unauthorized Data Access When It Contracted With DOH And During Performance Of The Contract**

---

64. Defendant knowingly failed to obtain secure and confidential computer programs and systems, before it contracted with DOH. Defendant knew that its system was not secure because it never purchased or installed data management security programs. Defendant then performed under the DOH contract without placing adequate safety controls on the data, programs and system.

65. Ms. Seilkop obtained contact tracers' response sheets, which should have contained lines of data necessary to prepare contact tracing reports. Ms. Seilkop's job was to merge this data into a report and aggregate the data, creating pivot tables<sup>6</sup> as needed to present the data.

---

<sup>6</sup> From the Microsoft website: A PivotTable is an interactive way to quickly summarize large amounts of data. PivotTables can be used to query large amounts of data; summarize data by categories and subcategories; provide details from the summary data for areas of interest; move rows to columns or columns to rows (or "pivoting") to see different summaries of the source data; filtering, sorting, and grouping the most useful

66. Ms. Seilkop asked McKay how to obtain the Covid tracing data in order to aggregate the data. McKay told her that the data was stored in Google Docs, and that he would have the username and password sent to Ms. Seilkop. McKay explained that each individual Google Doc document had its own username and password. There were three Google Docs documents used by workers, and three usernames and passwords shared by the workers.

67. Ms. Seilkop told McKay that this system, one username and password for each Google Docs document, and the workers' use of shared usernames and passwords to access Google Docs documents, was dangerous, not secure, and failed to protect confidential information. Ms. Seilkop also told McKay that Google Docs, a free, unsecure system, was incapable of protecting patients' confidential information.

68. Ms. Seilkop's statements notified Defendant, by and through McKay, that its actions constituted a potential data breach and therefore a reportable violation of the contract.

69. McKay ignored Ms. Seilkop's statements about the lack of security, stating that Defendant did not want to spend the money required to purchase secure software and install security measures in its computer systems in order to ensure the security of the DOH project information and confidential data. It was well known among Defendant's

---

subset of data enabling the user to focus on the information sought; and presenting concise, attractive, and annotated online or printed reports.

workers that Defendant would not purchase secure systems to protect confidential information.

70. McKay told Ms. Seilkop that Defendant was unwilling to purchase the data security components, and instead was using its DOH funds to hire workers. Defendant made a profit from the hourly rates paid to contact tracers and other workers.<sup>7</sup>

71. Under the contract, DOH paid Defendant for time and materials. The contract did not specify the types of data security required to perform the contract. If Defendant could have been paid for its acquisition of data security materials or programs (plus overhead and profit), it is more likely than not that Defendant would have purchased such materials if for no other reason than to make a profit on those purchases. Instead, Defendant stated that it would not spend any money on data security programs and instead would use its funds to hire workers.

72. Defendant also knowingly staffed the DOH project with managers who did not have IT and data system experience or the ability to create secure systems. From the beginning of her employment, it was clear to Ms. Seilkop that Defendant's managers did not understand the importance of data security.

73. From her first days working for Defendant, it was also clear to Ms. Seilkop that

---

<sup>7</sup> Defendant paid Ms. Seilkop less than half of what Defendant charged DOH for her services.

Defendant had used Google Docs as the repository of its data since the project began in July 2020.

74. In late October 2020, Ms. Seilkop told McKay that Defendant's use of Google Docs was unsecure and permitted anyone who accessed the program to see any other user's personal, private, saved usernames and passwords. This system also permitted a user's data from other Google related accounts<sup>8</sup> to be visible to anyone logged on to the system. McKay did not respond to this comment.

75. Ms. Seilkop also told McKay in October 2020 that the new computers it supplied to its workers were all delivered with Microsoft accounts already loaded, permitting Defendant to create a secure network of Microsoft email accounts. Ms. Seilkop told McKay that, if all workers were required to create a work email account using Microsoft Outlook, with an Insight superuser, Defendant would have an added level of security which did not exist in the current system. McKay did not respond to Ms. Seilkop's suggestion, but McKay never required Insight to create a Microsoft Outlook

---

<sup>8</sup> In addition to Google Docs, Google also offers multiple applications (apps), most for free, that transfer data between each other and permit access using one username and password. Access to a Google username and password will provide large amounts of information about the person's multiple Google apps accounts, and the ability to see what the user had recently accessed on the internet. Among other things, Google offers an email program (Gmail); a free and/or paid cloud storage site (Google Cloud); a calendar app (Google Calendar); three instant messaging accounts for personal communication (Google Duo, Chat and Meeting); Google Maps, Waze, Google Earth and Street View (mapping and navigation sites that track a user's current location) and note taking apps (Google Keep and Jamboard).

system for email security or workers to create Microsoft email accounts, or to change their current work system of one username and password for all staff.

76. Ms. Seilkop continued working for Defendant but remained concerned about the lack of security and controls on the data being processed. Ms. Seilkop continued to witness the dangers of the Defendant's system, and as a normal part of her job saw exposed data, from both patient PHI and PII data and coworkers' PII data that had been saved, and was accessible, in the only repository available to contact tracers, Google Docs.

77. In early December 2020, unable to obtain any responses to her complaints from McKay or from other managers, Ms. Seilkop contacted the Insight recruiter who had placed her, Jeffrey Lison, seeking his assistance in contacting Defendant's management about the serious deficiencies in the DOH contract performance. Ms. Seilkop explained to Lison the serious dangers inherent in Defendant's DOH data programs and systems (or lack thereof), but Mr. Lison did not understand the technicalities of the computer issues.

78. On or around December 14, 2020, Ms. Seilkop wrote an email to Lison explaining in detail her concerns regarding Defendant's lack of data security and safety protections for its DOH program and systems that stored PHI and PII. Ms. Seilkop told Lison that these security breaches were serious, and that she needed to speak to someone in Defendant's management who would understand how its DOH data storage violated its

obligations to DOH. This is the second instance in which Ms. Seilkop notified Defendant that its dangerous and insecure data system, a violation of the contract, resulted in a potential data breach. Defendant again failed to notify DOH of a potential data breach.

79. Lison forwarded her email to four of Defendant's employees, including manager McKay. Shortly thereafter, Ms. Seilkop's invitations to business meetings were rescinded, and she was isolated from both work meetings and coworker interactions.

80. Ms. Seilkop then emailed Lison again, stating that she could not continue working for Defendant if McKay and others refused to work with her. Within thirty minutes of that email, McKay called Ms. Seilkop and demanded to know why she voiced her complaints to Lison. McKay stated that her complaints made him look incompetent.

81. Ms. Seilkop again explained to McKay the dangers of the unsecure, easily accessible data stored on Google Docs and the dangers of only using one password. McKay denied that Ms. Seilkop's claims were true. Ms. Seilkop then sent McKay screen shots she had taken of other workers' accounts that were easily accessible through Google Docs, supporting her claims that the Defendant's programs and systems were not secure and permitted easy access to confidential data.

82. McKay told Ms. Seilkop that he was stunned by her ability to obtain these screen shots and would fix this problem. McKay's solution to the unsecure system was to create one new username and password for each Google Docs document. McKay also permitted all of Defendant's workers to share the new usernames and passwords.

83. This is the third instance where Ms. Seilkop notified Defendant that its unsecure data storage resulted in a potential data breach. Defendant again failed to notify DOH of the potential data breach.

84. After her conversation with McKay, Defendant continued to isolate Ms. Seilkop in her work. She was excluded from work meetings, and invitations that she had received were deleted.

85. Approximately two weeks later, Ms. Seilkop accessed Google Docs and saw that no new data was populated into the forms. Manager Shannon Hughes told Ms. Seilkop that Defendant was now storing its data on Microsoft applications, instead of Google Docs, in a "hub." No one had notified Ms. Seilkop, the person responsible for aggregating the data for DOH reports, of this change. However, Defendant continued the practice of one username and password per document, for all of the workers to share.

86. McKay had notified workers about this switch from Google Docs to Microsoft using Slack, providing employees with a link on Slack to the new Microsoft document storage site. Again, Defendant failed to heed its contractually obligated data safety requirements by sharing a link to a confidential document site on an unsecure messaging app.

87. This new Microsoft data storage system provided more security than Google Docs but still resulted in security failures that were never resolved. Workers were still accessing this site using unsecure email, since McKay never required workers to switch

to Microsoft Outlook accounts.<sup>9</sup> Workers were accessing this site using the three usernames and passwords provided.

88. Moreover, even after its switch to the Microsoft hub, Defendant failed to secure the data created prior to January 1, 2021. This original data was still in Google Docs. No additional security was added to the Google Docs platform to ensure safe storage of the previously obtained confidential information.

89. Despite being aware of its security failures at the contract's inception, Defendant never informed DOH, or its own employees, of its failure to secure data, or of the high likelihood of a data breach. Instead, Defendant continued allegedly performing under the contract as if all of the data was secure. In fact, throughout the contract performance, the data was unsecure and readily accessible by unapproved users.

**B. Defendant Failed To Track Data In A Valid, Relevant or Useful Manner, Resulting In Worthless Data Reporting To DOH**

90. Defendant's method of tracking Covid-19 data was not within acceptable data tracking or management standards, resulting in a complete failure to track data in a valid, relevant or useful manner. As a result, the reports created from this data were worthless.

91. Ms. Seilkop's job involved aggregating data from over one thousand contact tracers to produce valid, relevant, searchable data and reports for DOH. When she started working for Defendant, contact tracers used a form with questions and blank spaces

---

<sup>9</sup> Microsoft Outlook email accounts add a level of security because Outlook can be controlled by the employer, who can create and manage security for all users.

where contact tracers were to record responses to questions. There were at least thirty categories of questions for contact tracers to ask patients

92. Ensuring that the completed forms contained reliable, valid, relevant and searchable data depended upon the questioning and typing skills of each individual contact tracer.

93. In order for data to be searchable and trackable, and therefore be useful for public health purposes, data collection forms must contain a means of standardizing responses, so that contact tracers filling the forms could use pre-set and pre-populated responses each time. Prepopulated responses permit categories of information to be tracked across multiple response forms. For instance, if a patient was questioned about whether their initial symptoms included a fever, and the patient stated that they had a fever for three days, a contact tracer would need to record that a three-day fever had occurred. A pre-set and pre-populated form would contain a dropdown box that would record the existence of a fever, and that it lasted for three days.

94. Once dropdown boxes are created for each line of questioning, such as the fever example above, the contact tracer's recording of preset data corresponding to the patient's responses creates data that can be aggregated, and compiled, so that reports can be run from the data. These types of reports provide the ultimate user with the ability to determine trends in pathogen spread and management. For instance, if the aggregated and compiled data showed that a particular percentage of Pennsylvania's Covid-19 patients

had fever for three days, such data may help DOH and the Federal government in its predictions and treatment of Covid-19 cases.

95. Defendant's contact tracing forms were never valid, relevant, or usable. The forms contained blank spaces where contact tracers failed to record responses to questions. Many responses that were entered contained incorrect spelling, or unintelligible symbols or abbreviations. Thus, a search for a word, for example "fever," would not pull data related to fever where the word had been misspelled or simply not entered. Accordingly, it was undeterminable how many responses would have properly shown that a fever had occurred, let alone how long a fever was present. As a result of Defendant's failure to use basic data management processes, any searches run on this data would not produce valid results.

96. Ms. Seilkop's job required her to create reports on multiple data variables in order to report that data to DOH. For instance, Ms. Seilkop regularly ran a search, and created a report, on the top five Covid-19 symptoms. The reports resulting from these searches were meaningless because the searches would only catch symptoms a tracer had manually inserted and spelled correctly. The "top five symptoms" searches only caught those symptoms that had most often been correctly recorded, not the symptoms that occurred most often.

97. Ms. Seilkop shared her concerns with McKay about the lack of meaningful

data. McKay did not understand Ms. Seilkop's concerns, as he had no experience in data management. Ms. Seilkop voiced her concerns that the data should not be shared with DOH because it was not useful or accurate for reporting to the DOH in its current state. Despite having been informed of its worthlessness, McKay asked Ms. Seilkop to create pivot tables from this worthless data.<sup>10</sup> Ms. Seilkop did as she was asked, but McKay was unhappy with Ms. Seilkop's tables as he was unable to open the pivot tables on his cell phone. McKay directed Ms. Seilkop to take screen shots of the pivot tables so that he could see the pivot tables on his cell phone.

98. When Defendant transitioned to Microsoft spreadsheets, it began creating a contact tracing form that contained some dropdown boxes. The new forms were created by persons with no formal IT or data management training, including Defendant's social support coordinators.

99. The new form did not create dropdown boxes for all of the questions required to track and trace Covid-19. The new form still produced data that did not permit valid, relevant or useful searches.

100. Ms. Seilkop, one of the only people on the DOH project with data management experience, was excluded from the team that created the new form. In fact, some of the social support coordinators tasked with creating the new form apologized to Ms. Seilkop,

---

<sup>10</sup> Ms. Seilkop used Pivot Tables to visualize data responses by creating charts, graphs, and presentations. But since the data was invalid and unusable, the pivot table charts, graphs and presentation were similarly invalid and unusable.

telling her that McKay had recruited them to create the new form because Defendant allegedly had no employees with technical training who were capable of creating such forms.

101. Defendant knowingly directed social support coordinators to create the contact tracing form instead of paying data management professionals such as Ms. Seilkop to create a form that would permit valid, relevant or useful searches to occur and allow for valid, relevant and useful data reporting.

102. Defendant then submitted worthless data to DOH, claiming it was the result of its contracted services for the provision of Covid-19 contact tracing data. The information submitted was based on invalid data, making the reported results invalid, irrelevant, and worthless.

**C. Defendant Constructively Discharged Ms. Seilkop**

103. Ms. Seilkop reported to her supervisor, and to other Defendant managers, that Defendant was violating its contract and the law when it failed to securely manage PHI and PII, and failed to create valid, useful, relevant data.

104. Ms. Seilkop took lawful acts in furtherance of an action under the False Claims Act. Ms. Seilkop put her employer on notice of her protected activity.

105. Once Ms. Seilkop reported these violations she was harassed, ostracized and discriminated against in the terms and conditions of her employment by McKay, and other Defendant managers, in that they intentionally removed her job responsibilities,

restricted her interactions with other workers, and ultimately constructively discharged Ms. Seilkop. Ms. Seilkop was harassed by McKay, who yelled at her for reporting violations.

106. Unable to continue working for a company that intentionally failed to secure confidential patient information, knowingly failed to collect valid, useful or relevant data, or a company that harassed her when she internally blew the whistle, Ms. Seilkop was constructively discharged on January 8, 2021.

## **VI. LEGAL CAUSES OF ACTION**

### **COUNT I Violations Of The False Claims Act 31 U.S.C. § (a)(1)(A)**

107. Plaintiff incorporates by reference paragraphs 1 through 102 as though set out at length herein.

108. By virtue of the acts described above, Defendant knowingly caused to be presented, a false or fraudulent claim for payment or approval to the United States.

109. The Defendant's false or fraudulent claims were material to the Government's payment decisions.

110. The United States, unaware of the foregoing circumstances and conduct, and in

reliance on the truth and accuracy of the claims submitted for payment, paid or authorized payment of those claims and has been damaged in an amount to be proven at trial.

**COUNT II**  
**Violations Of The False Claims Act**  
**31 U.S.C. (a)(1)(B)**

111. Plaintiff incorporates by reference paragraphs 1 through 102 as though set out at length herein.

112. Defendant knowingly made, used, or caused to be made or used, a false record or statement material to a false or fraudulent claim submitted to the United States.

113. The United States, unaware of the foregoing circumstances and conduct, and in reliance on the truth and accuracy of the false records or statements submitted for payment, paid or authorized payment of those claims and has been damaged in an amount to be proven at trial.

**COUNT III**  
**Plaintiff Terralyn Williams Seilkop v. Defendant**  
**Violations Of The False Claims Act**  
**31 U.S.C. § 3730(h)**

114. Plaintiff incorporates by reference paragraphs 1 through 106 as though set out at length herein.

115. Plaintiff took lawful acts in furtherance of an action under the False Claims

Act.

116. Plaintiff put her employer on notice of her protected activity.

117. As a result of her lawful acts, Plaintiff was threatened, harassed, terminated and discriminated against in the terms and conditions of her employment.

118. As a result of her lawful acts, Plaintiff suffered damages, including but not limited to emotional distress.

## **VII. PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff demands that judgment be entered in favor of the United States and herself and against Defendant for the maximum amount of damages and such other relief as the Court may deem appropriate on each Count.

This includes, with respect to the FCA, three times the amount of damages to the United States plus civil penalties of no more than \$23,331 and no less than \$11,665 for each violation occurring after November 2, 2015; and any other recoveries or relief provided for under the FCA or by law.

Further, Relator requests that she receive the maximum amount permitted by law from the proceeds or settlement of this action as well as from any alternative remedies collected by the United States, plus reasonable expenses necessarily incurred, and reasonable attorneys' fees and costs. Relator requests that her award be based upon the

total value recovered, both tangible and intangible, including any amounts received from individuals or entities who are not parties to this action.

Further, Relator demands that judgement be entered in her favor and against Defendant under 31 U.S.C. § 3730(h), and that she receive the maximum amount of damages provided in the statute, including reinstatement with the same seniority status that she would have had but for the discrimination, 2 times the amount of back pay, interest on the back pay, and compensation for any special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys' fees.

#### **DEMAND FOR JURY TRIAL**

A jury trial is demanded in this case.

July 29, 2021

Respectfully submitted,

COHEN MILSTEIN SELLERS &  
TOLL, PLLC

By: /s/ Regina D. Poserina

---

Regina D. Poserina

Gary L. Azorsky

Jeanne A. Markey

Regina D. Poserina

3 Logan Square, 1717 Arch Street  
Suite 3610

Philadelphia, PA 19103

(267) 479-5700

[gazorsky@cohenmilstein.com](mailto:gazorsky@cohenmilstein.com)

[jmarkey@cohenmilstein.com](mailto:jmarkey@cohenmilstein.com)

[rposerina@cohenmilstein.com](mailto:rposerina@cohenmilstein.com)

*Attorneys for Relator*

*Terralyn Williams Seilkop*

## **CERTIFICATE OF SERVICE**

I hereby certify that on July 29, 2021, I filed, via paper filing, the Complaint and Motion to Seal the Action, with the Clerk of the Court, and in turn I served a true and correct copy of such documents upon the following:

The Hon. Merrick B. Garland  
United States Attorney General  
United States Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530

Bruce D. Brandler  
Acting United States Attorney  
Office of the United States Attorney for the  
Middle District of Pennsylvania  
Harrisburg Federal Building and Courthouse  
228 Walnut Street, Suite 220  
P.O. Box 11754  
Harrisburg, PA 17108-1754

Dated: July 29, 2021

/s/ Regina D. Poserina  
\_\_\_\_\_  
Regina D. Poserina